DARKTRACE

Blackhawk Network

Overview

Industry

○ Financial Services

Challenge

○ Use of several tools proving inefficient and cumbersome

○ Insufficiency of rules and signature-based approaches

○ Needed to reduce noise from network

○ Wanted a tool to stay on top of fast-evolving threats

Results

○ Increased efficiency by switching to Enterprise Immune System

○ Transitioned security stack to emphasize 'immune system' approach

○ Gives 100% real time threat detection and visualization

○ Confidence in security stack to detect zero-day threats

Business Background

Based in Pleasanton, California, Blackhawk Network is a globally-recognized company that pioneered 'branded value', providing solutions like gift cards, digital payments, and loyalty points. Its programs combine unique branded value content with business services to engage consumers across networks, from in-store, to B2B, to loyalty programs.

> " We previously needed three tools to tell us what Darktrace tells us on its own. The machine learning capabilities have saved us so much time, measuring the scope of what needs to be done, and it's spotting things that signature-based approaches are missing. "
>
> **Vari Bindra, Head of Cyber Defense Center, Blackhawk Network**

Challenge

As a growing company that is rapidly expanding into the international market, Blackhawk Network was concerned about the evolving threat landscape that jeopardized its sensitive personal and partner information. It felt that increasingly sophisticated attackers may target its private data with the potential to seriously damage the company's premier reputation. Further, Blackhawk Network wanted a solution that could visualize all insider traffic, in real time, without capturing all of the noise in a corporate network. It needed to look at only the most important threats, and devote its time to mitigating them as they emerged, before damage could be done.

Additionally, Blackhawk Network found that its existing security stack was proving inefficient. It was using three separate tools for threat detection and visibility, all using rules and signatures. "Using three separate tools proved inadequate for our security team," commented Vari Bindra, Head of Cyber Defense Center, Blackhawk Network. "It was very time-consuming to use all of the different tools, and we were concerned about staying on top of new threats, given our tools all used prior assumptions of 'bad'."

Solution

In an effort to reduce the noise of the network, stay on top of rapidly-evolving threats, and improve visibility and efficiency, Blackhawk Network deployed Darktrace's Enterprise Immune System in the heart of the network. Powered by unsupervised machine learning and advancements in Bayesian mathematics, the Enterprise Immune System can establish a 'pattern of life' for every network, device, and user, as soon as it's installed. With the probabilistic understanding of abnormality, potential cyber-threats are detected as they emerge, before they escalate into crisis.

"A machine learning approach is critical to cyber defense," Bindra commented. "The self-learning technology only focuses on the most important threats and finds abnormalities without any prior assumptions". Blackhawk Network further saw the value in the Enterprise Immune System as the Threat Visualizer provided a total overview of all insider traffic, which could be followed in real time on the 3D graphical interface. "We can scale up or down the number of abnormalities, or potential threats, we want to work on, "added Bindra. "Darktrace's Threat Visualizer makes it simple and easy to understand what is actually happening inside of our network."

In addition, the Enterprise Immune System's innovative technology is always learning what is 'normal' for the network, allowing it to grow with the company as it expands internationally. Even in this time of transition, Darktrace detects new threats.

Benefits

Thanks to the Enterprise Immune System's unique self-learning technology, Blackhawk Network has unparalleled visibility and awareness of its entire network. Because Darktrace determines the level of threat associated with each anomaly, false positives are filtered out and the security team is only notified of the most pressing potential attacks via the Threat Visualizer. Additionally, Blackhawk Network stays on top of the evolving threat landscape, as Darktrace is agnostic to threat type - it uses no rules, signatures, or prior assumptions.

Blackhawk Network also reduced their security stack to use only the Enterprise Immune System for threat detection and visibility, helping to reduce the burden on the security team. "Darktrace's Enterprise Immune System has increased efficiency tenfold," commented Bindra. "We previously needed three tools to tell us what Darktrace tells us on its own. The machine learning capabilities have saved us so much time, measuring the scope of what needs to be done, and it's spotting things that signature-based approaches are missing".

By basing its security strategy on self-learning technology, Blackhawk Network has increased its confidence to keep its private data secured from the inside of the network, even as it grows and expands into the international market. Blackhawk Network has proven itself as an industry leader as the Enterprise Immune System allows it to remain proactive and efficient against the most advanced forms of cyber-threat.

> "
>
> [Darktrace] was created with an analyst in mind, not just a slap-on technology on top of an analyst's already busy world.
>
> "
>
> **Vari Bindra, Head of Cyber Defense Center, Blackhawk Network**